EXERCICE 8 — Gestion des risques liés aux tiers & à la supply chain

Contexte professionnel

ShopNow dépend de plusieurs tiers :

- C6 / A3 : prestataire de paiement (Stripe),
- CDN / hébergeur,
- éventuels services d'emailing, d'analytics, etc.

Les attaques supply chain et la compromission de prestataires sont un risque majeur.

Objectifs pédagogiques

L'étudiant doit être capable de :

- Identifier les **dépendances critiques**.
- Évaluer les **risques liés aux tiers**.
- Proposer des **mesures contractuelles, techniques et organisationnelles**.
- Intégrer ces risques dans la vision globale Security by Design / Zero Trust.

Consigne générale

Rapport en anglais (page de garde, sommaire, numérotation, conclusion).

Travail demandé

1. **Cartographie des tiers**

Listez les tiers critiques (au moins 4, dont Stripe) :

| Tiers | Rôle | Données traitées | Impact en cas de compromission | Menaces STRIDE dominantes |

2. **Analyse de risques supply chain**

Pour chaque tiers :

    - Risques techniques (compromission API, fuite de données, indisponibilité),
    - Risques contractuels (absence de SLA, absence de clauses sécurité),
    - Risques de conformité (RGPD, localisation des données).

3. **Mesures de maîtrise**

Proposez des mesures :

    - **Contractuelles** : clauses de sécurité, audits, SLA, notification d'incident.

- **Techniques** : segmentation réseau, tokens limités, scopes restreints, rotation de clés, monitoring des appels.
- **Organisationnelles** : revue périodique des prestataires, processus de due diligence.

Sous forme de tableau :

| Tiers | Risque principal | Mesure proposée | Priorité | Responsable interne |

4. **Intégration dans Zero Trust**
    - Expliquez comment traiter les tiers comme des **zones externes non fiables** :
        - authentification forte,
        - limitation des permissions,
        - vérification systématique des réponses.

5. Quel tiers représente le **risque le plus critique** pour ShopNow ?

6. Quelles actions doivent être engagées **immédiatement** ?

ANNEXE A — Tiers critiques

Tiers	Rôle	Données
Stripe	Paiement	D6
CDN	Fichiers statiques	C1
Hébergeur	Infra	C2, C3
Email provider	Notifications	D1

ANNEXE B — Risques supply chain

- Compromission API
- Indisponibilité prestataire
- Mauvaise configuration
- Absence de SLA
- Fuite de données
- Dépendance excessive

ANNEXE C — Mesures de maîtrise

- Contrats : SLA, clauses sécurité
- Techniques : rotation clés, scopes limités
- Organisation : audits, due diligence
- Zero Trust : pas de confiance implicite